**DEPARTMENT OF THE ARMY**
**MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND**
**200 STOVALL STREET**
**ALEXANDRIA, VA 22332-5000**

SDG6 (25)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: SDDC Password Policy

1. Reference AR 25-2, Information Assurance, para 4-12, 14 Nov 03.

2. The reference above mandates a system password protection policy to protect the organization's information systems. SDDC commanders must ensure that assigned personnel are knowledgeable of the password requirements in this policy and that adherence to this policy is strictly enforced.

3. The majority of intrusions of information systems have been accomplished with a compromised password. Passwords can be compromised with a password cracker tool or by social engineering. Social engineering exploits the human vulnerability of a system rather than attacking the system. Potential hackers may pose as individuals that would have a legitimate reason for access, (i.e., help desk personnel or systems administrators). These hackers may call a user and ask for their password, gain access to work areas to look for passwords written in obvious locations, or engage in "dumpster diving", checking office waste for user lists, computer printouts or passwords written on scrap paper.

4. It is imperative that access is controlled and the following procedures are implemented immediately to ensure protection of passwords and official information.

a. Passwords will be protected at the same level of the information they are used to protect but never lower than sensitive but unclassified (SBU). Passwords will be changed every 90 days at a minimum for all information systems.

b. Passwords will be a mix of upper case letters, lower case letters, numbers and special characters and will be at least 10 characters in length. The password must contain at least two characters from each set. Users will not use a dictionary word as a password. The numeric characters will not be dates or any other sequence that may be associated with the user, office, or system. The password will not be the same as the user ID.

SDDC (25)
SUBJECT: SDDC Password Policy

c. Users having access to multiple systems will have a different password for each system. In case one password is compromised, it will not allow access to all systems. Specifically this applies to users with SIPRNET and NIPRNET accounts. See enclosure for specific examples.

d. Those systems that have password storage and repetition checking will not allow the reuse of a password within 10 changes.

e. All information systems with password aging capability will be set to force the user to change passwords every 90 days.

f. Users will not disclose or share their password for any reason. Systems administrators, technical help desk personnel and supervisors do not have a legitimate reason for knowing any users passwords and will not ask for it. Passwords will not be written down and left within the work area. Any copies of access information produced by systems (i.e., printouts, diskettes, backup tapes) will be destroyed in accordance with sensitivity of the system, SBU or classified.

g. If a user has any reason to believe that their password has been compromised, they will change it immediately and report the incident to the systems administrator and the Information Assurance Office.

5. POC for this action is Ms. Kimberly Quinn, IAPM, 703-428-2128, DSN 328-2128 email quinnk@sddc.army.mil.

Encl

ANN E. DUNWOODY
Major General, USA
Commanding

DISTRIBUTION:
Deputy Commanding General, SDDC, 661Sheppard Place, Fort Eustis, VA 23604-5000
Director, SDDC Transportation Engineering Agency, 720 Thimble Shoals Blvd, Suite 130, Newport News, VA 23606-2574
Commander, 597th Transportation Group, Military Ocean Terminal Sunny Point, 6280 Sunny Point Road, Southport, NC 28461-5000
Commander, 598th Transportation Group, Unit 6713, Box 173, APO AE 09709
Commander, 599th Transportation Group, Bldg 204, Wheeler AAF, Schofield Barracks, HI 96857-5008
HQ SDDC Staff Principals

**THE RULES**

**Passwords must consist of *at least* ten *characters* with *at least two characters from each* of the following *four sets...***

**SET 1:** a b c d e f g h i j k l m n o p q r s t u v w x y z

**S E T 2 :** A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

**SET3:** 0123456789

**SET 4:** . - !@#$%*()-+[{]}\I;:‘“,<.>/?

In addition to using a character from each of the above sets, a good password MUST NOT contain a plain text word:

*BAD PASSWORD EXAMPLE:* yelLowSO#

GOOD *PASSWORD EXAMPLE:* Dp239@$sH2

Additionally, DO NOT USE:

- A proper name, especially your own, the name of family members, pets or favorite sports teams. ( Ex. John, dog, Steelers, Rams)

- A dictionary word. (Ex. work, password (yes believe it or not some people have used “password”)

- A common word that may not be in the dictionary but still easily recognized.( Ex. Pokemon, Blitzen, CISCO, )

- A hybrid dictionary word. A hybrid dictionary word builds upon a dictionary word by adding or modifying with numeric and symbol characters. (Ex. Bogus1 1 or Annaliza!!)

Following the guidance above in constructing your password will significantly reduce the risk of a poor password being cracked and subsequently being used to compromise our network. Taking the time to properly construct a good password is essential to assisting MTMC in defending our network. **Always beware of phone calls or e-mail from hackers posing as network administrators...never, never give your password to anyone over the phone or by e-mail.**

(3)